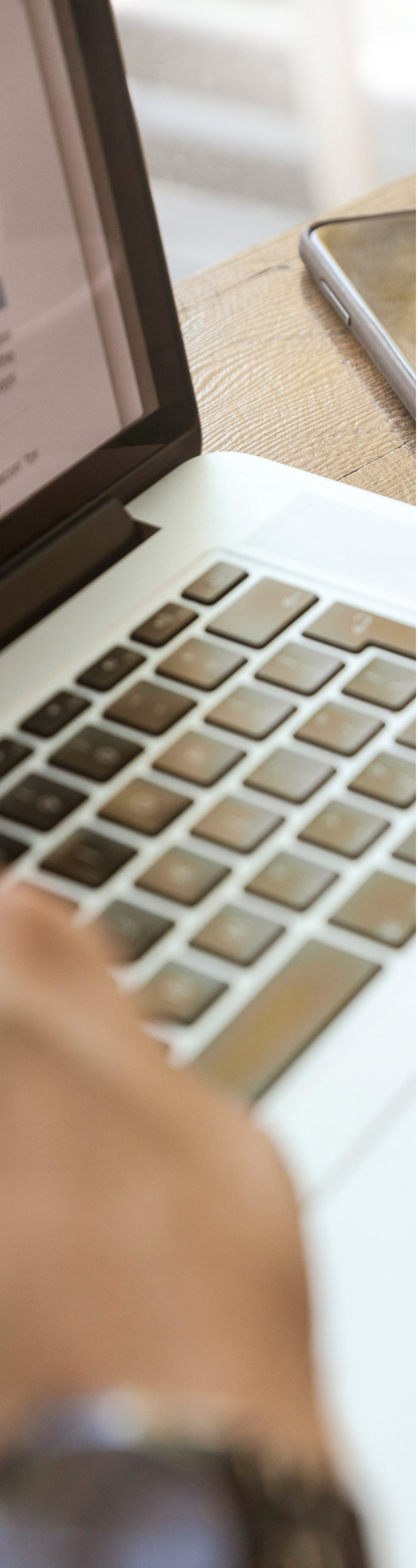
AVOCAR
Comunicação

SEGURANÇA NA

INTERNET

AVOCAR COMUNICAÇÃO

SEGURANÇA NA INTERNET



CAPÍTULO 1

COMO NAVEGAR COM SEGURANÇA

1 | COMO NAVEGAR COM SEGURANÇA

O Brasil é um dos países com maior número de crimes cibernéticos. Em 2018 passamos a ocupar o segundo lugar na ocorrência desses delitos. De acordo com a associação SaferNet Brasil, nesse período foram registradas 133.732 queixas, frente a 63.698 em 2017. Fruto da popularização dos smartphones, o mundo virtual virou paraíso de hackers e outros tipos de criminosos. Eles buscam limpar contas bancárias, devassar a vida privada, roubar senhas e arquivos pessoais. Estão atentos a tudo que possa ser usado para extorquir suas vítimas. Mais de 25% dos casos de violação de segurança em empresas são fruto de falhas humanas.

É possível se prevenir de possíveis ataques seguindo algumas medidas de segurança.

1. Ao acessar seu e-mail, conta, perfil de rede social ou Internet banking em um computador de uso público saia clicando “Logout”, “Sair”, “Desconectar” ou algo equivalente

2. Crie senhas difíceis de serem descobertas. Prefira sequências que misturem letras, números ou símbolos. Mude as senhas periodicamente e não as guarde em arquivos de texto

3. Use versões atuais de navegadores, com correções contra falhas de segurança. Atualize seu antivírus, inclusive em tablets e smartphones

4. Cuidado com downloads. Sempre verifique se o arquivo não possui características estranhas como extensões desconhecidas ou tamanho muito pequeno

5. Evite clicar em anúncios duvidosos, como os pop-ups que aparecem no computador ou no smartphone. Eles são responsáveis por vários problemas com vírus e danos de segurança

6. Não use softwares piratas ou acesse sites duvidosos. Desconfie ou ignore links sobre dívidas, prêmios, traição conjugal, solicitação de dados bancário

7. Cuidado com os anexos de e-mails anunciando “fotos comprometedoras” ou outro chamariz hiperbólico. Eles podem espalhar malwares. Cheque os arquivos com antivírus

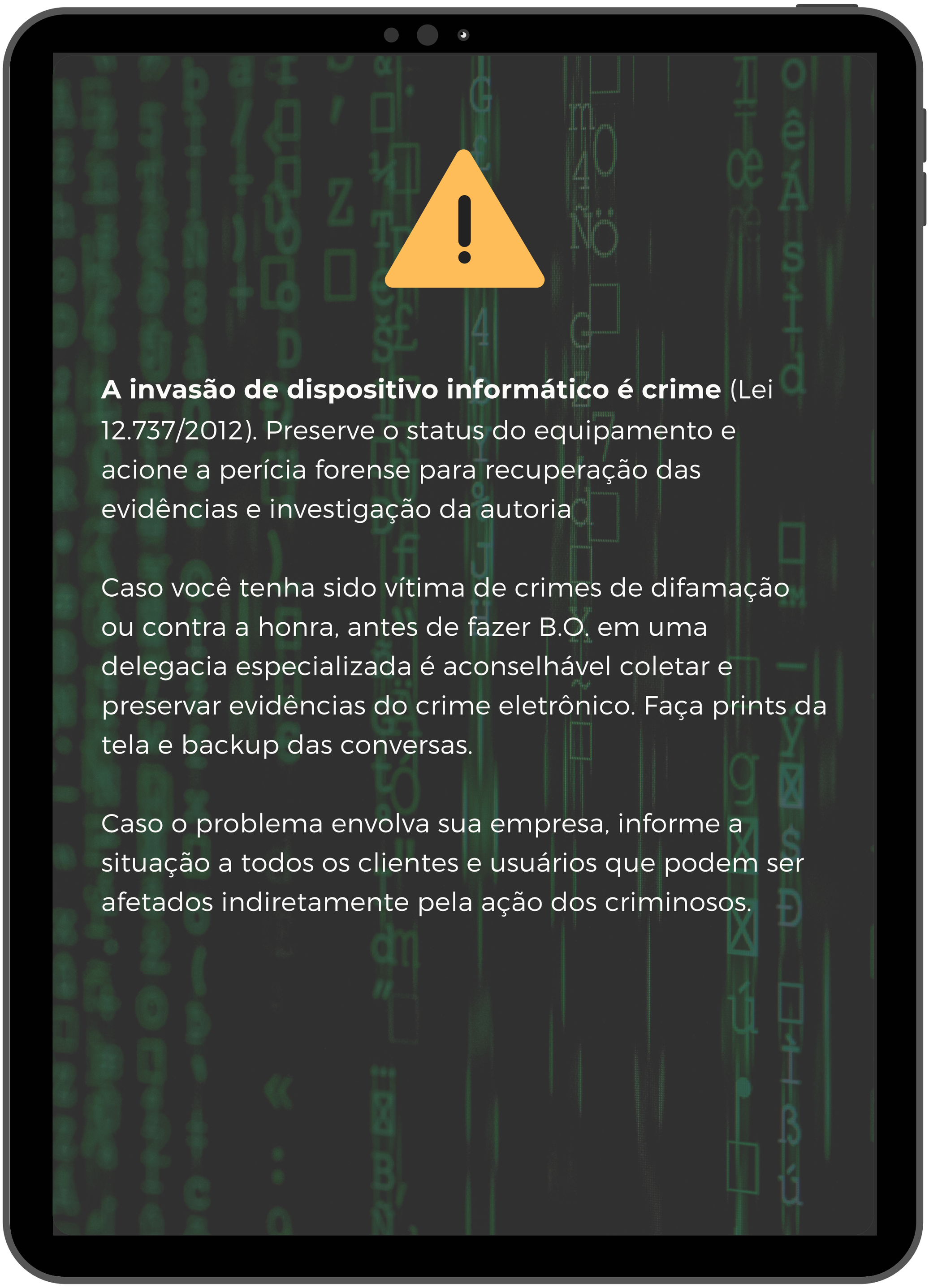
8. Atenção ao comprar pela internet. Escolha sites de lojas de boa reputação. Verifique se o site possui Certificado de Segurança checando se a URL dele começa com https://

9. Não responda a ameaças, provocações ou intimidações. Se perceber que a ameaça é séria, procure uma delegacia especializada em crimes cibernéticos

10. Nunca revele nas redes sociais dados ou informações relevantes ou privadas sobre você e sua família. Caso necessário, faça-o de forma privada

11. Opte por serviços que ofereçam a opção de verificação em duas etapas por meio de um código enviado por SMS. Assim, com sua senha, não conseguirão acessar sua conta

13. Assista a vídeos em sites conhecidos. Garanta que programas como Flash e Java estejam atualizados – versões antigas facilitam o acesso para atacarem o seu computador



A invasão de dispositivo informático é crime (Lei 12.737/2012). Preserve o status do equipamento e acione a perícia forense para recuperação das evidências e investigação da autoria

Caso você tenha sido vítima de crimes de difamação ou contra a honra, antes de fazer B.O. em uma delegacia especializada é aconselhável coletar e preservar evidências do crime eletrônico. Faça prints da tela e backup das conversas.

Caso o problema envolva sua empresa, informe a situação a todos os clientes e usuários que podem ser afetados indiretamente pela ação dos criminosos.

CAPÍTULO 2

WHATSAPP

O WhatsApp tornou-se um dos aplicativos de troca de mensagens de texto, imagem e voz mais populares do mundo. Nem por isso deve ter suas ameaças subestimadas. Pelo fato de a troca de mensagens ser geralmente pessoal, ninguém quer um desconhecido lendo o que foi escrito; nem que os dados trocados no aplicativo caiam nas mãos de um criminoso virtual.
Veja o que fazer para evitar problemas:

Os avanços das redes sociais trouxeram consigo novos desafios para seus usuários. Alguns deles relacionam-se às providências a serem tomadas contra os crimes cibernéticos e à legislação aplicável contra eles.
Caso seus contatos relatem o recebimento de mensagens estranhas vindas do seu número, sua conta pode ter sido clonada.
Saiba o que fazer em dois casos frequentes:

CLONAGEM DE CHIP

- Para recuperar sua conta, registre um B.O. (Boletim de Ocorrência)
- Informe os familiares e contatos sobre a clonagem
- Ligue para a operadora e bloqueie o chip
- Solicite o bloqueio da conta de usuário pelo e-mail support@whatsapp.com
- Adquira um novo chip na loja física da operadora
- Inicie a conta no WhatsApp com novo código recebido via SMS
- Caso o criminoso tenha habilitado uma verificação em 2ª etapa:
  Após a recuperação da conta, digite de forma errada os códigos sucessivos para suspender a conta por sete dias. Após esse período, registre a conta novamente. Você receberá, via SMS, um novo código de ativação.

CLONAGEM DA CONTA

- Registre um B.O
- Avise contatos e parentes
- Envie um e-mail para support@whatsapp.com. No campo “assunto” escreva: Perdido/Roubado: “Desative minha conta”. No corpo da mensagem informe seu telefone com o código do país. O WhatsApp desativará sua conta por sete dias
- Após o criminoso habilitar a verificação em duas etapas, reinstale o número do aplicativo e digite de forma errada os códigos sucessivos até bloquear a conta. Você receberá um novo SMS

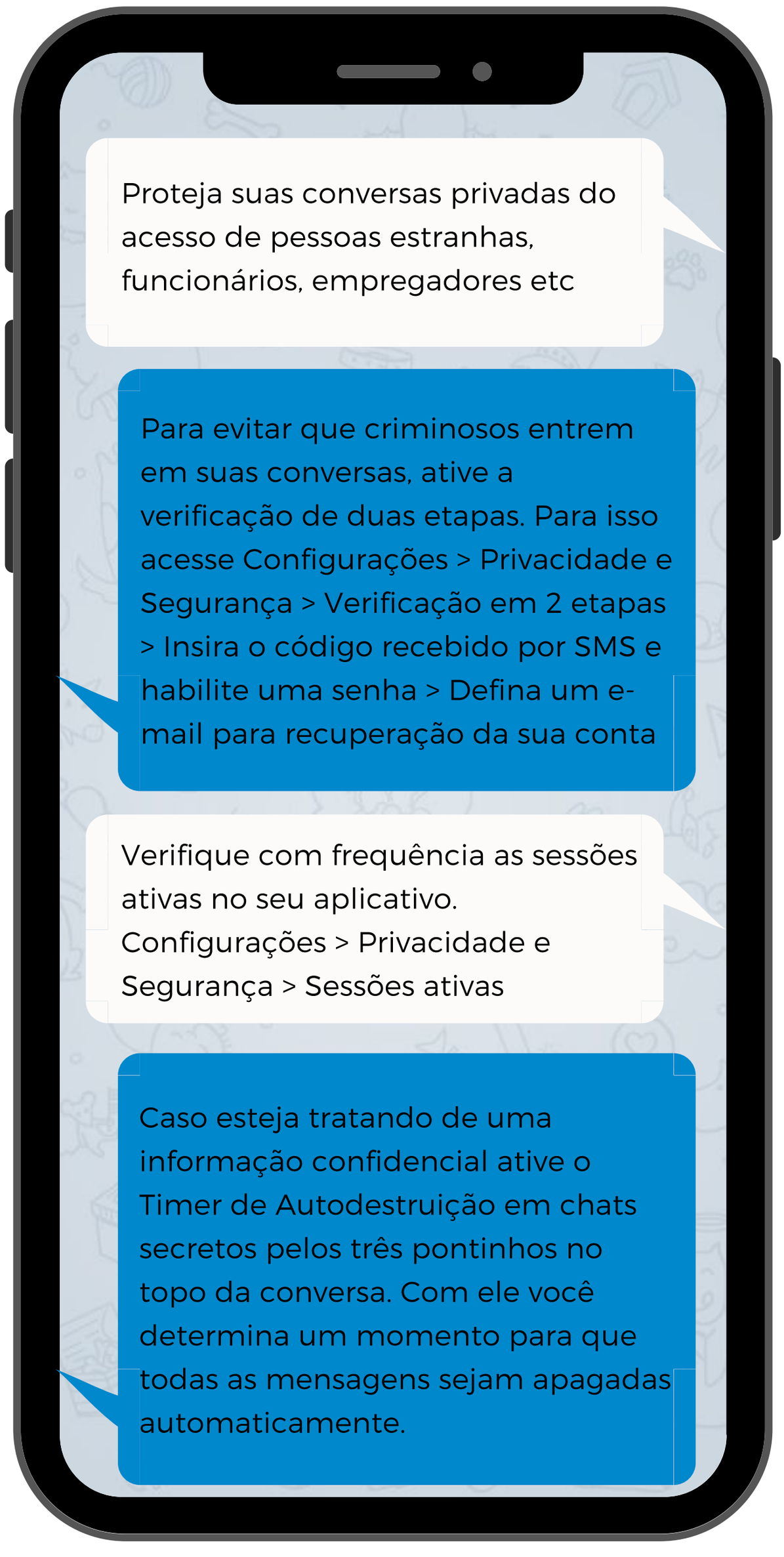
CAPÍTULO 3

TELEGRAM

3 | TELEGRAM

O Telegram é um aplicativo de mensagens muito rápido, simples e gratuito. Você pode usá-lo em todos os seus dispositivos ao mesmo tempo — suas mensagens serão sincronizadas em todos os seus celulares, tablets ou computadores. Além de mensagens, você pode enviar fotos, vídeos e arquivos de qualquer tipo (doc, zip, mp3, etc). Pode ainda criar grupos de até 200 mil pessoas ou canais para transmitir para audiências ilimitadas. Permite conversar com seus contatos telefônicos ou procura-los pelo nome de usuário.

Para alguns especialistas, o Telegram é mais seguro do que o WhatsApp. As mensagens são guardadas na nuvem, em servidores da empresa espalhados pelo mundo. O Telegram também possui um chat secreto e, de acordo com a empresa, esse serviço oferece máxima privacidade ao usuário. Nesse modo, as mensagens são protegidas por criptografia passo-a-passo desde que saem do remetente até chegarem ao interlocutor, mas nessa modalidade, não é possível criar grupos. Porém, nenhum aplicativo é totalmente seguro. É necessário, então, tomar alguns cuidados em relação à privacidade:



O Telegram traz uma opção nativa que bloqueia o acesso ao aplicativo por meio de uma senha criada por você

Com isso, não é preciso se preocupar se alguém vai visualizar uma mensagem em seu celular de forma indevida, pois será preciso informar o código para abrir o app

Há ainda uma função de autodestruição da conta. Nela, seu perfil e todos os seus dados serão apagados caso você fique sem acessar o aplicativo durante um determinado período ou tenha sido invadido em seu conteúdo.

Atenção: você determina esse intervalo de tempo para que aconteça a autodestruição

CAPÍTULO 4

FACEBOOK

Mais de 130 milhões de brasileiros estão no Facebook. Perto de 90% deles acessam a rede social por dispositivos móveis, principalmente no celular. Nem todos os espaços virtuais são confiáveis. Por isso, todo o cuidado é pouco com o conteúdo postado.
Veja algumas providências para manter sua conta segura:

Proteja sua senha. Não use sua senha do Facebook em outro local online. Nunca compartilhe sua senha. Ela deve ser difícil de adivinhar com no mínimo seis números, letras e símbolos gráficos. Evite incluir o seu nome ou palavras comuns.

Cuidado com o que você publica. Algumas pessoas se expõem demais, postando fotos de casa, pertences, viagens. Em alguns casos chegam a informar quando estarão viajando, dando assim as dicas para que pessoas mal-intencionadas possam agir.

Não clique em tudo que aparece na tela. Cuidado ao clicar em links sugeridos, até mesmo por amigos. Pessoas criam perfis falsos e se aproveitam para mandar vírus que podem danificar seu computador, ou até roubar senhas e se apoderar de seu perfil.

Informações financeiras ou compra de bens não devem ser expostas, pois representam uma porta aberta e um convite para criminosos. Evite comentários como dizer que pegou fila em seu banco, revelando rotinas de sua vida financeira. Evite ostentações.

Cuidado ao postar opiniões ou críticas sobre pessoas em geral. Caso sintam-se ofendidas, elas podem utilizar sua postagem como prova de injuria ou difamação. O mesmo se aplica no caso de incitação à violência ou declarações de ódio e preconceito.

Utilize os recursos extras de segurança do Facebook como a Autenticação de dois fatores. Acesse Configurações > Segurança e Login e veja todas as opções para manter sua conta segura.

Saia da sua conta no Facebook ao usar um computador compartilhado. Caso se esqueça, há a opção de sair remotamente. Não marque a caixa “Mantenha-me conectado” ao efetuar login em um computador público.

Em casos de ameaça moral, física ou pública é possível atribuir a autoria de delitos praticados nas redes sociais. Para tanto, você deve agir de maneira oportuna e preservar as postagens ofensivas.

- A pessoa que o ofendeu poderá ser identificada por meio da URL, username, ID, e-mail ou telefone

- Preserve o conteúdo ofensivo. Isso pode ser feito por meio de certidão lavrada por escrivão de polícia ou da Plataforma Records, disponível em www.facebook.com/records. O mesmo endereço pode ser utilizado – apenas pelos órgãos encarregados da investigação – para encaminhar ordens judiciais e requisição de dados cadastrais

- Em casos que envolvam perigo de morte ou lesão grave, a polícia pode requisitar, independentemente de ordem judicial, por meio da Plataforma Records, os dados que levem à identificação do responsável pelas ameaças e, assim, coibi-las. Caso não haja riscos, a polícia poderá solicitar a expedição de uma ordem judicial sobre fornecimento de informações

- Qualquer pessoa pode denunciar ameaças à segurança pública ou pessoal de terceiros

- A conta de um usuário do Facebook falecido pode ser transformada em um memorial. Pode ainda ser excluída por meio de solicitação de parente ou representante legal. O conteúdo dessa conta será acessado apenas por pessoas compartilhadas. Em sua página inicial é utilizada a expressão “Em memória”. Não estarão registrados em tais perfis lembretes de aniversário. Seu conteúdo não poderá ser exibido em espaços públicos

CAPÍTULO 5

INSTAGRAM

5 | INSTAGRAM

O Instagram é uma das mais populares redes sociais de fotos. No Brasil, consolidou-se como a segunda em preferência para quem quer ganhar seguidores ou divulgar seu negócio. Essa rede é gratuita e, a partir dela, é possível tirar fotos com o celular, aplicar efeitos nas imagens e compartilhar com seus amigos. Conheça algumas maneiras para utilizá-la bem e com segurança.

Utilize uma senha forte, pessoal e intransferível. Prefira uma combinação de, no mínimo, seis números, letras e pontuações. A senha também deve ser diferente daquelas usadas por você em outros locais da Internet

Mude sua senha com frequência, especialmente se você receber uma mensagem do Instagram solicitando para alterá-la

Nunca informe sua senha para pessoas desconhecidas ou para quem não seja de sua inteira confiança

Ative a autenticação de dois fatores para obter segurança extra para a conta.
Acesse Configurações > Segurança > Autentificação de dois fatores

Veja se sua conta de e-mail está segura. Possivelmente, qualquer pessoa que tenha acesso a seus e-mails também terá acesso à sua conta do Instagram

Saia de sua conta ao usar um computador ou celular compartilhado. Não marque a caixa “Mantenha-me conectado” ao efetuar login em um computador público

Evite spam, aquelas mensagens não solicitadas para pessoas que não se interessam por seu produto ou perfil. Portanto, evite seguir perfis aleatórios apenas para que eles sigam você

Pense bem antes de autorizar aplicativos de terceiros

Se você for bloqueado abra o aplicativo do Instagram no seu celular e na tela de acesso, toque em “Obter ajuda para entrar”; Informe o nome de usuário, telefone ou e-mail de cadastro (para achar sua conta); Toque em “Avançar” e você verá uma nova tela, já com a foto do seu perfil; Toque em “Enviar e-mail” e terá acesso a um link para recuperar a conta

Se não funcionar ou o Instagram não encontrar mais a sua conta (porque o invasor mudou o nome de usuário, e-mail e outros detalhes), siga novamente até a etapa anterior e toque em “Precisa de mais ajuda?”. A partir daí você vai denunciar que sua conta foi invadida e enviar a solicitação ao suporte (que entra em contato por e-mail)

Casos de chantagem no Instagram, por parte de pessoas que acessam de forma não autorizada fotos ou dados, podem ser denunciados em uma página do aplicativo. A pessoa com quem você está se comunicando não será notificada

Você também pode denunciar a postagem de fotos de teor violento, cunho erótico/sexual ou de apologia a distúrbios alimentares etc. Ao encontrar tal imagem, acesse-a e clique no ícone com os três pontinhos. Surge um menu de opções. Selecione a opção que melhor se enquadrar à sua queixa

Denúncia de conta de pessoa falecida – caso você veja uma conta que pertence a alguém que faleceu, poderá registrar o fato para que a rede faça um memorial. Se você é parente direto dessa pessoa, também pode solicitar que a conta seja removida. Basta preencher um formulário na página do Instagram. Após o envio de solicitação de remoção da conta, a rede social pede provas de que você é parente direto da pessoa falecida

CAPÍTULO 6

LINKEDIN

O LinkedIn é uma rede em expansão, atualmente está presente em cerca de 200 países. O foco do Linkedin – diferentemente de outras plataformas – é manter relações corporativas e contatos de trabalho. Nessa rede você conecta recrutadores e candidatos em busca de emprego. Mas, para criar um perfil de sucesso na rede, é preciso seguir alguns passos e evitar ciladas:

Mude sua senha periodicamente. Não a utilize em todos os sites que você acessa. Faça escolhas com no mínimo 6 caracteres, difíceis de serem adivinhados. Nunca forneça a senha a terceiros, nem a anote em arquivos do Word ou em outro aplicativo

Saia de sua conta após utilizar computadores de uso público. Não marque a caixa “Mantenha-me conectado” ao efetuar login em um computador público. Isso o manterá conectado mesmo depois de fechar a janela do navegador

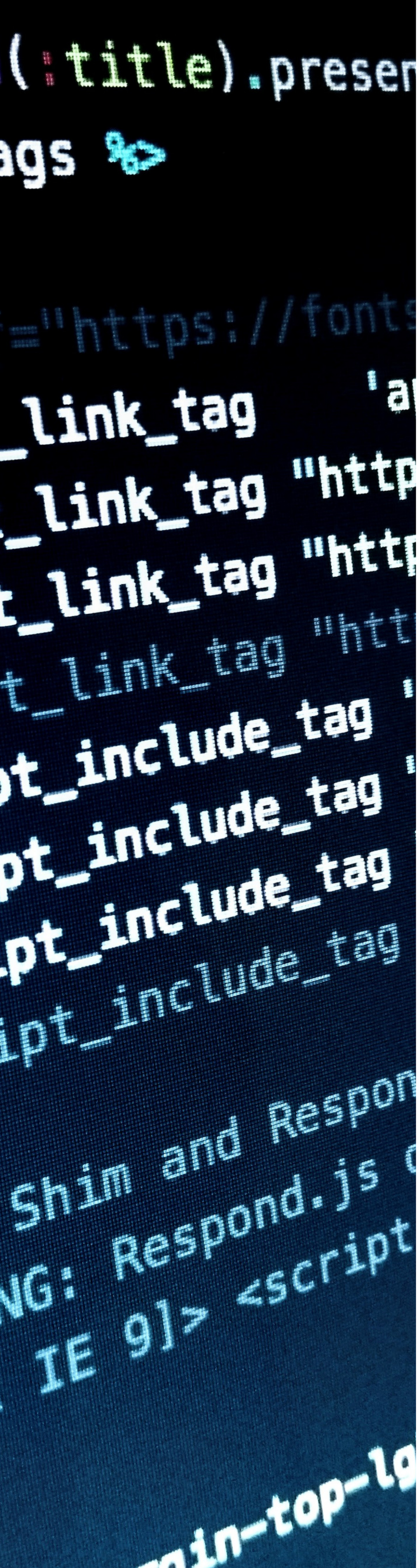
Gerencie as configurações de privacidade e informações da sua conta na página “Configurações e privacidade”

Ative em sua conta a verificação em duas etapas. Acesse Eu > Configurações e Privacidade > Conta > Acesso e segurança > Verficação em duas etapas

O próprio Linkedin, em sua página de Ajuda, oferece orientações caso você queira fazer alguma denúncia de mensagens ou imagens inadequadas ou problemas de segurança. A empresa oferece uma maneira de marcar o conteúdo diretamente no site

Assédios ou utilização de linguagem hostil podem ser denunciados e bloqueados. No que concerne a conteúdos inadequados no SlideShare, a empresa orienta a que você marque o conteúdo inconveniente e comprometa-se a enviar a denúncia para seu setor de segurança e confiança, que realizará uma revisão

Após avaliar os itens denunciados, a empresa compromete-se a exclui-los caso se constate um crime. O Linkedin garante a privacidade do denunciante. Porém, a empresa alerta que possui capacidade limitada de ação no que se refere ao conteúdo exibido fora do site, a menos que se trate de uma violação direta de sua marca



CAPÍTULO 7

CIBERCRIMES

Crimes cibernéticos são todos os delitos cometidos por meio de computadores ou da internet em redes públicas, privadas ou domésticas. Os objetivos desses variam de acordo com os interesses do criminoso. As formas de cometer também são diversas e podem atingir apenas um usuário, vários deles, ou inclusive um sistema de redes completo.

Conhecer exemplos dessas práticas pode auxiliar a entender o que são atividades ilegais cibernéticas e como se proteger delas. Os exemplos mais comuns ficam por conta dos vírus de computador, programas e códigos maliciosos, roubo de informações, fraude de dados, além de acessos não autorizados.

Também existem os crimes conhecidos como tradicionais ou comuns, que usam a internet como instrumento: bullying, intimidação, chantagem, calúnia, assédio, extorsão, espionagem, plágios, pornografia infantil e terrorismo, entre outros.

2/3 dos adultos do mundo foram vítimas de cibercrimes

Algumas das formas mais comuns desses crimes cibernéticos envolve o envio de e-mails com vírus, mensagens em redes sociais, além de roubo de informações por meio de sites de bancos e de comércio eletrônico.

O Relatório de Crimes Cibernéticos Norton, empresa de segurança na Internet, aponta que quase dois terços dos adultos, em todo o mundo, já foram vítimas de algum tipo de crime cibernético (65%). A China lidera o ranking (83%). Brasil e Índia registram 76% e EUA somam 73%.

Brasil: computadores infectados

Vírus de computadores e ataques de malware são os tipos mais comuns de crimes cibernéticos. Na Nova Zelândia, Brasil e China são mais de seis em cada 10 computadores infectados (61%, 62% e 65%, respectivamente). Os adultos também são alvos de golpes (scams) online, ataques de phishing, roubo de perfis de redes sociais e fraude de cartão de crédito. 7% dos adultos se depararam com predadores sexuais online.

62% dos computadores no Brasil já foram infectados

86% dos usuários temem os crimes cibernéticos

44% das vítimas ligam para a polícia

Segundo o estudo da Norton, 86% dos usuários temem os crimes cibernéticos. Apenas 3% dos entrevistados pensam que jamais sofrerão crimes cibernéticos. Ainda assim, apenas 51% afirmam que mudariam a forma de se comportar online caso se tornassem vítimas. Das pessoas ouvidas, 56% atribuem a culpa pelos delitos a delinquentes anônimos e 21% ao crime organizado.

Quando os delitos cibernéticos ocorrem, menos da metade das vítimas entra em contato com seu banco (48%). Outros 44% ligam para a polícia e apenas 34% entram em contato com o proprietário do website ou do provedor.

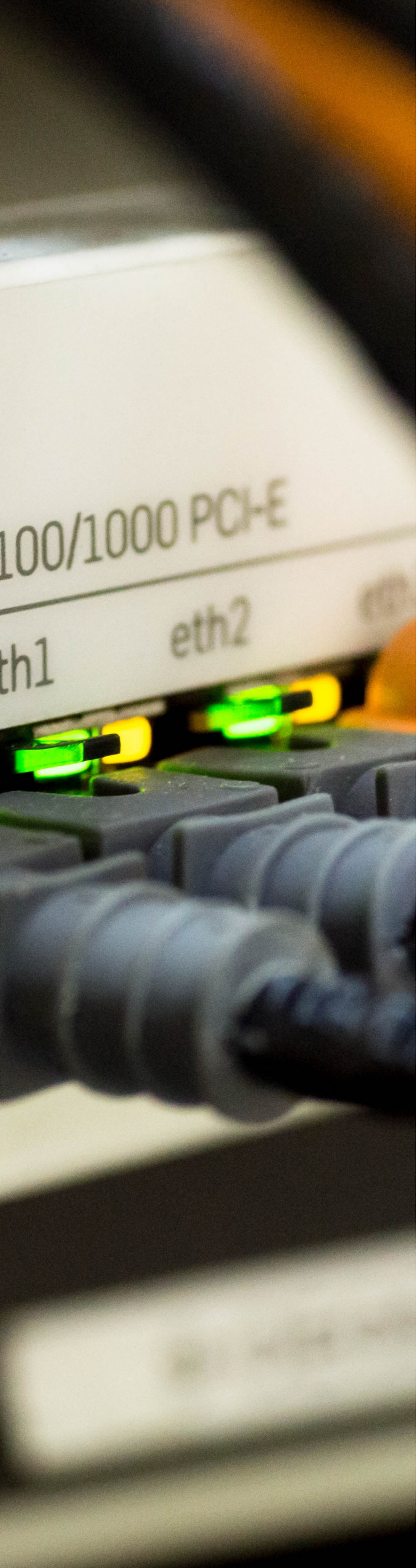
Impacto financeiro

Um dos impactos mais sentidos se relaciona às finanças. Em 2018, essa modalidade de crime provocou prejuízo de o equivalente a R$ 3 bilhões, segundo a PF (Polícia Federal). A maior parte diz respeito a fraudes bancárias. Por outro lado, a PF sofre com a falta de delegacias especializadas e a utilização de computadores ultrapassados. O setor de cibercrimes possui apenas 20 funcionários – os EUA têm 1,2 mil agentes especializados.

Além do impacto financeiro, para 28% das vítimas o maior incômodo relaciona-se ao tempo de resolução – são consumidas até quatro semanas em caso de crime cibernético comum. Há também os danos emocionais: 19% se disseram estressadas, raivosas ou constrangidas. Pelo menos 14% lamentaram a perda de dados insubstituíveis ou itens de valor sentimental, como fotos e vídeos. O pior é que 31% afirmam que nunca conseguiram resolver o problema.

Embora a maioria das pessoas não se veja como um criminoso digital, 17% consideram “legal” baixar uma faixa musical, álbum (14%) ou filme (15%) sem pagar. Apenas 22% dos usuários afirmam estar arrependidos por causa dessas práticas. O estudo indica ainda que quase metade de todas as pessoas fica feliz em contar mentiras online sobre seus detalhes pessoais, incluindo nome, idade, situação financeira, estado civil, sua aparência e até mesmo sua nacionalidade. Ao menos 33% dos adultos já assumiram identidades falsas online – desde um nome falso até uma identidade totalmente fictícia. Cerca de 40% dos italianos, brasileiros e neozelandeses já usaram identidades falsas .

Mas há o lado bom da moeda. O estudo sugere que as pessoas entendem que ser um bom cidadão digital tem tudo a ver com respeito. Regras pessoais, etiqueta online e boas maneiras são semelhantes em todo o mundo. Apenas uma minoria (2%) não tem quaisquer regras. E boa parte está se mexendo para combater os cibercrimes. Pelo menos 75% nunca fornecem suas senhas, não prestam informações pessoais sem necessidade (73%), não abrem anexos/links de estranhos (71%), tomam cuidado com as ofertas “muito boas para ser verdade” (69%) e mantêm detalhes financeiros seguros (69%).



CAPÍTULO 8

MARCO CIVIL DA INTERNET

O Marco Civil da Internet (MCI) é uma espécie de Constituição do mundo digital brasileiro. Sancionado pela então presidente Dilma Rousseff, em 23 de abril de 2014, por meio da Lei 12.965/14, define regras e assegura direitos e deveres dos usuários e das empresas que atuam no mundo digital e são provedoras de acesso e de serviços online.

O MCI foi criado para garantir a mesma qualidade de acesso à rede para todos, sem distinção. Proíbe provedores de telecomunicações de restringir conexão e velocidade, dependendo do conteúdo, origem, destino e serviço acessado pelo internauta. Isso impede, por exemplo, a cobrança de tarifas diferenciadas de acordo com a qualidade do serviço prestado.

Por exemplo, é proibido barrar o Spotify e liberar a Netflix, propiciar uma velocidade ao Twitter e outra ao Facebook. A ideia do MCI é que o usuário tenha acesso a toda a internet, e não a aplicativos, serviços ou sites pré-determinados pelo provedor.

Quanto à guarda e registro de acessos, a lei estabelece a obrigação de que estes itens sejam atribuições do provedor do serviço, que deve armazenar tais registros por no mínimo 1 (um) ano.

Danos de conteúdos gerados a terceiros

O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. Esta seção da lei também trata sobre possíveis acordos gerados pela publicação de conteúdo relacionado a honra, reputação ou direitos de personalidade, bem como sobre a indisponibilização desses conteúdos, por provedores de aplicações de internet, quando conveniente.

ENTRE OS DIREITOS ESTIPULADOS PELA LEI ESTÃO:

A obrigatoriedade da retirada de conteúdos ofensivos de sites, blogs ou redes sociais. A determinação acorre por ordem judicial e responde ao delito quem produziu ou divulgou o material

A proteção e privacidade de dados do usuário na internet, incluindo e-mails e chats, que podem ser violadas apenas durante investigações criminais

Sites são obrigados a coletar dados com consentimento do usuário (que deve ser informado com clareza sobre como eles serão utilizados). É proibido passar essas informações para outras pessoas não autorizadas a recebê-las

A lei determina ainda que as mesmas normas de proteção e defesa do Código do Consumidor valem para compras e vendas feitas na internet

SÃO DEVERES PREVISTOS PELO MARCO CIVIL DA INTERNET:

O respeito à intimidade ou à vida privada de outros usuários e a proibição de divulgar ou compartilhar mensagens, vídeos ou imagens ofensivas a essas pessoas

Garantir a proibição de negócios virtuais ilícitos, como comercialização de armas de fogo, drogas, medicamentos, bem como a venda de produtos sem nota fiscal ou manual de instruções

Respeitar os direitos autorais. A reprodução de conteúdo (musical, literário, audiovisual etc.) sem autorização pode ser penalizada

Em caso de investigação, empresas de telecomunicações, portais e redes sociais devem identificar os usuários acusados por infringirem o MCI. Nesses casos, o direito à privacidade e à proteção de dados é suspenso

AVOCAR COMUNICAÇÃO

SEGURANÇA NA INTERNET

TEXTO | José Antonio Leite

REVISÃO | Equipe Avocar

EDIÇÃO | Júlia Faria

AVOCAR
Comunicação